REMARKS

Prior to entry of the present Amendment, claims 48-76 were pending in the application, with claims 1-47 having previously been cancelled without prejudice. In the present Amendment, claims 48, 57-59 and 76 are amended, and new claims 77-80 are added. No new matter is added.

Examiner's Interview

On October 28, 2009, Applicants' representative met with Examiner Tran and Examiner Apple. Applicants appreciate the Examiners' time and consideration during the Interview. During the Interview, Applicants' representative and the Examiners discussed proposed amended claims 48 and 76 and the cited prior art (including U.S. Patent Application Publication No. 2002/0178112 ("Goeller") and U.S. Patent No. 6,073,140 ("Morgan")). As discussed below in more detail, the Examiners suggested language to overcome the rejections under 35 U.S.C. §101, and the suggested language has been incorporated into amended claim 76. As also discussed below in more detail, Applicants' representative presented reasons as to why the claims overcome the cited prior art. While the Examiners agreed that the amended claims overcome the rejection under 35 U.S.C. §101 and appear to overcome the prior art rejection based on Goeller and Morgan, agreement was not reached on the claims.

Claim Rejections under 35 U.S.C. §101

The Examiner rejected claim 76 under 35 U.S.C. §101 as being directed to non-statutory subject matter. As mentioned above, the Examiners suggested language to overcome the rejection. Specifically, the Examiners suggested that acts of claim 76 be defined as being "on a computer". Applicants have amended claim 76 as suggested by the Examiners. Applicants submit that claim 76.is directed to statutory subject matter and, accordingly, respectfully request reconsideration of the rejections under 35 U.S.C. §101.

Claim Rejections under 35 U.S.C. §103

The Examiner rejected claims 48-76 under 35 U.S.C. §103 as being anticipated by Goeller in view of Morgan. For the reasons discussed during the Interview and below, Applicants respectfully request reconsideration of the rejections.

Independent Claim 48

Independent claim 48 defines a debit data validation system for a network, the system including a calling application configured to receive a request to validate debit data from a merchant, and receive transactional debit data that is to be validated; a debit data search engine including a keying module and a matching module, the debit data search engine being configured to receive the transactional debit data from the calling application, and to process the transactional debit data to identify a consumer key, the consumer key being based on at least a portion of the transactional debit data; and a debit data warehouse including stored debit data, the debit data warehouse being configured to retrieve the stored debit data associated with the consumer key, the stored debit data being representative of at least one consumer, and the consumer key linking the stored debit data gathered from a plurality of data sources. Claim 1 defines the calling application being further configured to process the stored debit data, to determine whether to allow the debit transaction, and to generate a response message to the merchant with the determination.

Goeller discloses a point of sale (POS) check service. In Goeller, a customer performs a transaction with a merchant and using a paper check for payment. Fig. 5; paragraph [0054]. In step 306, the customer presents a paper check for payment. Id. In step 310, the check is swiped through a device such as a MICR device. Fig. 5; paragraph [0055]. In step 322, additional customer information, such as driver's license number, state identification number, military identification number, etc., may entered into a device. Fig. 5; paragraph [0056].

In Goeller, a merchant may request that a check be converted, be verified and converted, or be guaranteed and converted. Fig. 6B; paragraph [0057]. If a merchant requests Conversion Only, the transaction will be approved or declined by a participating bank on which the check is drawn or by a third-party authorizing agent with minimal account verification processing. Id. If Conversion Only is requested, then the bank may merely check to see that a valid account does exist at the bank, that the account has not been closed, and that the account is not fraudulent. Paragraph [0066].

If a merchant is concerned about the authenticity of a check and wants to verify that funds are present in the customer's checking account at the time of purchase, the merchant may choose Verification with Conversion because there is a greater likelihood that the merchant will be paid. Paragraph [0058]. If the merchant chooses Verification with Conversion, a participating bank on which the check is drawn or an authorizing agent will verify the probability that the check will be paid based on information available at the time of the request. Paragraph

[0057]. When Verification with Conversion is requested, then in step 454 the bank not only verifies that the account is valid, but also that the amount of funds in the account is adequate for the transaction. Fig. 6B; paragraph [0066].

If a merchant wants guaranteed payment of the item, he may choose Guarantee with Conversion, in which case the guarantor bears the liability even if the check is not honored. Paragraph [0058]. If the merchant chooses the Guarantee with Conversion option, a participating bank on which the check is drawn or to an authorizing agent will guarantee the check. Fig. 6B; paragraph [0057]. If Guarantee with Conversion is desired, then in step 462 the bank will place a hold on the account for the amount of the transaction and will guarantee that the amount will be paid. Paragraph [0066].

As discussed during the Interview, Goeller does not teach or suggest, among other things, a debit data validation system including any component identifying a consumer key, the consumer key being based on at least a portion of the transactional debit data. Goeller also does not teach or suggest any component being configured to retrieve stored debit data associated with the consumer key, the stored debit data being representative of at least one consumer, the consumer key linking the stored debit data gathered from a plurality of data sources. At most, Goeller discloses that, based on information read from a check used in a transaction, a bank may not only verify that the checking account is valid, but also that the amount of funds in the checking account is adequate for the transaction.

Also, in Goeller, the verification will occur based on information available at the time of the request. There is nothing in Goeller to suggest that additional stored data is retrieved in the verification process or that such retrieved stored data is associated with a consumer key. In addition, Goeller does not teach or suggest any component being configured to process the stored debit data to determine whether to allow the debit transaction. Again, in Goeller, based on information read from a check used in a transaction, a bank may not only verify that the checking account is valid, but also that the amount of funds in the checking account is adequate for the transaction.

For at least these independent reasons, Goeller does not teach or suggest the subject matter defined by independent claim 48.

Morgan does not cure the deficiencies of Goeller. Morgan discloses a method and system for the creation, enhancement and update of remote data using persistent keys. Each persistent key uniquely identifies a particular data structure which may represent all the information known about a particular individual, a business, an address, a piece of real property,

or a vehicle. Col. 3, lines 53-57. When a data structure representing such an entity is stored both in a data vendor's central database and on a data customer's customer database, the persistent keys linked to each of these data structures will match, and this matching feature allows comparison of the equivalent data structures for efficient update or enhancement of data on the data customer's database. Id., lines 57-64.

In Morgan, the persistent keys are divided into several fields of information, including an entity code, a randomly-assigned unique number, and a version number. Fig. 5; col. 3, lines 65-67; see col. 10, line 55 through col. 11, line 27. The unique number is simply a randomly-assigned number to ensure that each persistent key is distinguishable from all other persistent keys. Col. 4, lines 6-8; see col. 11, lines 4-14.

In Morgan, a fundamental requirement of the disclosed invention is that each persistent key must be unique across the entire central database, and, thus, if two matching persistent keys are found, it may be assumed that these keys are linked to records with matching (but not necessarily identical) data. Col. 4, lines 8-13. The same unique number can be assigned to data structures representing different entities with related information, such as an individual and the address for that individual. Id., lines 13-17. The different entity code ensures that the overall persistent key for each data structure is unique, and the reuse of the same unique number for data structures with different entity codes allows, for example, the matching of an individual to that individual's vehicle using the persistent keys. Id., lines 17-22.

In Morgan, the process for data enhancement using persistent keys begins with the delivery to the data customer of a computer-readable medium containing the entire set of all persistent keys matched with a key field from the record associated with that persistent key. Id., lines 34-38; see col. 10, lines 13-26. The computer-readable medium also contains a software program that, when executed on the data customer's computer, matches the records in the data customer's database with the matching key field on the computer-readable medium, and, during this matching operation, the associated persistent key for each matched key field is copied onto the data customer's database and linked to the matched record. Col. 4, lines 46-52; see col. 10, lines 27-54. The initial key field matching process need only be performed once for any data customer's database. Col. 4, lines 65-66.

Once the persistent keys are incorporated into the data customer's database, in a batch mode method, the data customer need only supply the data vendor with a form indicating what data is requested along with the data customer's list of persistent keys. Col. 5, lines 7-14. Sending only the persistent keys to the data vendor, rather than all of the underlying data, is a

significant security advantage as well, since anyone who intercepts the list cannot extrapolate the underlying data from just a list of persistent keys. Id., lines 24-28.

In Morgan, the persistent keys also facilitate the linkage of the various physical databases that form the central database. Col. 6, lines 19-20. Data for related entities may be stored in numerous remote locations, requiring the central database manager to look in several locations to find all of the information requested by the data customer, and the central database manager uses the persistent keys to link this information together across physically remote databases. Id., lines 21-26.

As also discussed during the Interview, Morgan does not teach or suggest, among other things, a debit data validation system including any component identifying a consumer key, the consumer key being based on at least a portion of the transactional debit data. Morgan also does not teach or suggest any component being configured to retrieve stored debit data associated with the consumer key, the stored debit data being representative of at least one consumer, the consumer key linking the stored debit data gathered from a plurality of data sources. Instead, Morgan uses persistent keys to link data structures, and, rather than being based on at least a portion of transactional debit data, the persistent keys of Morgan are divided into several fields of information, including an entity code, a randomly-assigned unique number, and a version number. In fact, a significant security advantage of the persistent keys of Morgan is that anyone who intercepts a list of persistent cannot extrapolate any underlying data.

Also, Morgan does not teach or suggest a debit data validation system. Morgan merely discloses a method and system for the creation, enhancement and update of remote data using persistent keys and is not related to debit data validation. In addition, Morgan does not teach or suggest such a debit data validation system including a calling application, a debit data search engine, or a debit data warehouse, as claimed.

For at least these independent reasons, Morgan also does not teach or suggest the subject matter defined by independent claim 48.

Further, as discussed during the Interview, the references teach away from the proposed combination. The POS check service, disclosed by Goeller, would not and could not be modified to use the persistent keys to link data, as disclosed by Morgan.

As mentioned above, in the POS check service of Goeller, a customer performs a transaction with a merchant and using a paper check for payment, and a merchant may request that a check be converted, be verified and converted, or be guaranteed and converted. At most, in Goeller, if a merchant is concerned about the authenticity of a check and wants to verify that

funds are present in the customer's checking account at the time of purchase, a bank not only verifies that the account is valid, but also that the amount of funds in the account is adequate for the transaction based on information available at the time of the request.

In contrast, Morgan uses persistent keys, including an entity code, a randomly-assigned unique number, and a version number, to link data structures. In order to use the persistent keys of Morgan to match data, the associated persistent key for each matched key field must first be copied onto a data customer's database and linked to the matched record.

Therefore, in order to modify the POS check service disclosed by Goeller to use the persistent keys of Morgan, the merchant of Goeller would need to have a database of all its customers and, before performing any transactions, to first have the record for each and every customer in that database matched to a unique persistent key. Such requirements are unthinkable for a point of sale merchant. Also, even if a merchant did implement such a database, if a customer of Goeller is not in the database (likely a common occurrence for many merchants) and/or is not matched to a persistent key, the data linking of Morgan would not be possible. In addition, even if a merchant did implement the database, if a customer of Goeller is not the customer matched to a unique persistent key (for example, because the actual customer and the customer in the database have similar names, addresses, etc.), inaccurate data would be linked to the actual customer. For at least these independent reasons, the references teach away from such a combination.

In view of at least the foregoing, Goeller and Morgan, alone or in combination, do not teach or suggest the subject matter defined by independent claim 48. Accordingly, claim 48 is allowable. Dependent claims 49-75 and new dependent claims 77-80 depend from independent claim 48 and are allowable for at least the same and other independent reasons.

Independent Claim 76

Independent claim 76 defines a computer-implemented method of conducting a debit data validation of a consumer involved in a debit transaction, the method including receiving a request from a merchant to validate debit data of the consumer involved in a debit transaction; receiving transactional debit data that is to be validated; on a computer, retrieving a consumer key based on at least a portion of the transactional debit data, the consumer key linking debit data from a plurality of data sources; on a computer, analyzing the debit data associated with the consumer key; and, on a computer, generating a response message to the merchant, the response message being indicative of one of a first condition and a second condition, the first

condition being a validation of the debit data, and the second condition being a lack of validation of the debit data of the consumer.

As discussed during the Interview, Goeller does not teach or suggest, among other things, a computer-implemented method of conducting a debit data validation of a consumer involved in a debit transaction, the method including, on a computer, retrieving a consumer key based on at least a portion of the transactional debit data, the consumer key linking debit data from a plurality of data sources. At most, Goeller discloses that, based on information read from a check used in a transaction, a bank may not only verify that the checking account is valid, but also that the amount of funds in the checking account is adequate for the transaction.

Also, in Goeller, the verification will occur based on information available at the time of the request. There is nothing in Goeller to suggest debit data from a plurality of data sources is used in the verification process or that debit data is linked by a consumer key. In addition, Goeller does not teach or suggest, on a computer, analyzing the debit data associated with the consumer key. Again, in Goeller, based on information read from a check used in a transaction, a bank may not only verify that the checking account is valid, but also that the amount of funds in the checking account is adequate for the transaction.

For at least these independent reasons, Goeller does not teach or suggest the subject matter defined by independent claim 76.

Morgan does not cure the deficiencies of Goeller. As also discussed during the Interview, Morgan does not teach or suggest, among other things, a computer-implemented method of conducting a debit data validation of a consumer involved in a debit transaction, the method including, on a computer, retrieving a consumer key based on at least a portion of the transactional debit data. Instead, Morgan uses persistent keys to link data structures, and, rather than being based on at least a portion of transactional debit data, the persistent keys of Morgan are divided into several fields of information, including an entity code, a randomly-assigned unique number, and a version number. In fact, a significant security advantage of the persistent keys of Morgan is that anyone who intercepts a list of persistent cannot extrapolate any underlying data.

Also, Morgan does not teach or suggest a computer-implemented method of conducting a debit data validation of a consumer involved in a debit transaction. Morgan merely discloses a method and system for the creation, enhancement and update of remote data using persistent keys and is not related to debit data validation. In addition, Morgan does not teach or suggest such a method including receiving a request from a merchant to validate debit data, receiving

transactional debit data that is to be validated, on a computer, analyzing the debit data associated with the consumer key, or, on a computer, generating a response message to the merchant, as claimed.

For at least these independent reasons, Morgan also does not teach or suggest the subject matter defined by independent claim 76.

Further, as discussed during the Interview and above, the references teach away from the proposed combination. The POS check service, disclosed by Goeller, would not and could not be modified to use the persistent keys to link data, as disclosed by Morgan. Rather than represent the arguments set forth above with respect to this contention, for brevity's sake, Applicants refer to the discussion above for claim 48. With respect to claim 76, the same arguments apply.

In view of at least the foregoing, Goeller and Morgan, alone or in combination, do not teach or suggest the subject matter defined by independent claim 76. Accordingly, claim 76 is allowable.

CONCLUSION

In view of the foregoing, entry of the present Amendment and allowance of claims 48-80 are respectfully requested.

If additional consultation will further prosecution, the undersigned is available for telephone consultation during normal business hours.

Respectfully submitted,

/Edward R. Lawson Jr./

Edward R. Lawson Jr.
Reg. No. 41,931

File No. 025213-9075-00
Michael Best & Friedrich LLP
100 East Wisconsin Avenue, Suite 3300
Milwaukee, Wisconsin 53202-4108
414.271.6560